Quali-Sign Ltd

www.quali-sign.com

White Paper

Supporting a new communications API

Michael Adams

13th May 2016

Table of Contents

1 Background

Quali-Sign currently has a dependency on EBICS for communication. I.e. Quali-Sign performs the role of an 'EBICS Client'. It currently can only connect to 'EBICS Servers'. This is a pre-requisite on any bank or other institution / organisation that provides Quali-Sign to its customers, employees or counterparties as a means of capturing their authorisation signatures.

The EU's PSD2 legislation includes regulatory requirements to support 'Third Party Providers' connecting to banks or other Account Servicing Payment Service Provider's (ASPSP), via open standards API's.

The commission has tasked the EBA to publish '11 Technical Standards' (RTS), covering secure authentication and communication. These standards will be adopted into law by the commission.

At the time of writing of this paper, the EBA's draft RTS have not been published. This author is working on the assumption that the EBA will specify one of two options:-

a) The EBA will define a single communications standard, which all banks would be required to implement.
b) The EBA will define a shortlist of communications standards. As long as a bank implements one of the options, they will be deemed to have met the regulatory requirements.

All indications suggest that the second option is the most likely. If the EBA proceeds with this option, it is likely that EBICS will make the shortlist.

2 Purpose

The purpose of this document is to describe the minimum functional requirements (API's) of a new communication standard, as an alternative to EBICS. These would provide the equivalent functionality to allow Quali-Sign to operate without loss of capability.

3 Terminology

Please note: This document references banking terminology. However the functional requirements are applicable to other institutions / organisations.

EBICS calls its API's 'Orders'. These include 'Standard Orders' as well as what this author terms 'Banking Services'. Standard Orders support core functions, such as key management. Banking Services define specific (payment) initiation and reporting orders.

In terms of security keys, both the user and the bank have the following 3 keys:

a) Personal Authorisation Key
- This is the important key with respect to PSD2. When the user needs to apply a signature that is equivalent to their handwritten signature, this is the one they use.
- This key must have a corresponding Qualified Certificate, issued by a Qualified Trust Services Provider.

b) Identification and Authentication Key
- This key is used practically to sign a combination of the API message container and its payload. Therefore the recipient can prove that nothing has changed. It is used by the recipient to identify the submitter on receipt of the message. If the signature validation fails, the message is rejected.
- This key has a corresponding Self Signed Certificate.

c) Encryption Key
- This key is used to decrypt the payload in messages received from the sender. The sender encrypts the payload with the user's public key.
- This key has a corresponding Self Signed Certificate.

In the case of Quali-Sign, the above keys are locked into the Trusted Execution Environment of the mobile phone, which performs all the cryptographic functions on behalf of the app. To meet the regulations, the 'Personal Authorisation Key' must be secured with Knowledge (e.g. PIN) or Inheritance (Fingerprint). The other keys do not.

This separation means that Quali-Sign can be scheduled to communicate with the institution’s server, for example every 15 minutes, to download data. It will use the Identification and Authentication Key, plus the Encryption Key to do this. It does not need to use the Personal Authorisation Key. This key cannot be used as part of a background task as the owner of the device must physically unlock the key.

4 Functional Requirements

Before continuing, this author encourages you to watch the following demonstration video. It will help make sense of the requirements.

https://www.youtube.com/channel/UCkyfgl-D7Q6apb8qjM2B0PA

4.1 Initialize user with 'Certificate Signing Request'

- The first API to call if the user is not in possession of a Qualified Certificate.
- Used to transmit the user's 3 certificates to the bank. A CSR is transmitted in place of a Qualified Certificate for the Personal Authorisation Key.
- On receipt of these keys, the bank places the user in an 'Awaiting Activation' state, until they have received an 'Initialization Letter', documenting the 3 keys/certificates. The user must physically sign this letter in the presence of a bank official in order for the bank to issue a Qualified Certificate. Only once the certificate is issued will the user be activated.
- *Note: EBICS does not support CSR's today, a change request has been submitted with the EBICS Working Group. In the absence of this, Quali-Sign has implemented a workaround, the CSR approach would streamline the process.*

4.2 Initialize user with 'Qualified Certificate'

- The first API to call if the user has a Qualified Certificate.
- Transmits all 3 certificates to the bank.
- The bank needs to validate the (Qualified) certificate chain and check whether the certificate has not been revoked. This happens in real time.
- The user is activated by the bank without any manual intervention.

4.3 Download Bank Certificates

- Once the user has been activated, the bank will allow the user to download the bank certificates electronically.

4.4 Download 'Qualified Certificate'

- Now the user is active, they can download their certificate securely from the bank. They can then use this certificate with other institutions.
- *Note: there is currently not a corresponding EBICS Standard Order Type for this. A bespoke order type has been implemented.*

4.5 Suspend User

- This will reset the user back to a 'New' state on the bank's system.
- The user can use this if they are changing device and want to reinitialize on their new device.
- The user can also use it to suspend all communication with a particular bank, for a period of time.

4.6 Request new Qualified Certificate

- If the user has an active Qualified Certificate that will expire shortly, they are able to provision a new one electronically, without going through the manual process of signing a piece of paper and having this witnessed by a bank official.

4.7 Renew All Certificates

- User transmits their new Qualified Certificate, plus new Self Signed Certificates to the bank.

4.8 Renew Self Signed Certs

- User transmits new Self Signed Certificates for their 'Identification and Authentication Key' and their 'Encryption Key' to the bank.

4.9 Download User Permissions

- Download a list of Standard Orders and Banking Services that the user has access to.
- Also includes a list of accounts that they have access to.
- Includes permissions at a Banking Service / Account and Limit level.
- For 'Customer To Bank' (C2B) permissions, the user is assigned an 'Authorisation Level': E (highest level); A (second highest); B (third highest). Users with E class permissions can act as single signatory on orders that require a minimum of 1 signature. In all other cases, orders require 2 signatures.

4.10 Download Permissions for all Customer Users

- Similar to Download User Permissions. This order includes permissions for all users.
- Used by a customer 'super user'.

4.11 Acknowledgement

- On receipt of orders, some functions are performed by the bank asynchronously to the request. I.e. the user is not left hanging for the bank to perform its processing. In this case, it is possible that the request may get rejected at a later time. Calling the Acknowledgement order provides confirmation that the order was successfully processed. If rejected, reason information is provided.

4.12 List of new 'Bank to Customer' (B2C) orders awaiting download

- If the user has entitlements to download for a large number of different reports, this allows the user to call one order, which will tell them which (if any) new reports are available for download. They can then initiate a download for those specific reports, rather than initiating downloads for all the reports that they are registered for.

4.13 Requirements to support for multiple user signatures

4.13.1 List of C2B Banking Services awaiting authorisation

- Lists payment orders (for example) that have been transmitted to the bank but are awaiting additional signatures. The order will not be processed until these have been captured.

4.13.2 Download copy of C2B Banking Service

- This allows the authoriser to review the content of the (payment) order that they are being asked to approve. They can then decide whether to approve or send a cancellation request.

4.13.3 Approve C2B Banking Service

- Provide personal approval.

4.13.4 Request cancellation of C2B Banking Service

- Request cancellation.

5 Banking Services

5.1 Customer to Bank (C2B)

- Payment Initiation - Domestic Credit Transfer.
- Payment Initiation - SEPA Credit Transfer.
- Payment Initiation - Urgent, Cross Border, Cross Currency credit transfer.
- Payment Initiation - Intra-group Credit Transfer.
- Payment Initiation - Domestic Direct Debit.
- Payment Initiation - SEPA Direct Debit (Core).
- Payment Initiation - SEPA Direct Debit (B2B).

5.2 Bank to Customer (B2C)

Duplicate copies of the following banking services can be downloaded by supplying a date range. Otherwise only newly available reports are downloaded.

- Payment Initiation - Payment Status Report.
- Customer Account Maintenance - Daily Account Statement.
- Customer Account Maintenance - Intra-day Account Report.
- Customer Account Maintenance - Credit Advice.
- Customer Account Maintenance - Debit Advice.

6 Pre-requisites to implement a new communication standard

For new communication API's to be adopted, the following are required:-

- A detailed specification.
- A qualification environment to test against.